CLAIMS

What is claimed is:

1. A method of maintaining one or more lists of one or more network characteristics of a plurality of messages traveling near at least a first network node coupled to at least a first packet network, comprising:

detecting the plurality of messages traveling near at least the first network node coupled to at least the first packet network, wherein each of the plurality of messages comprises one or more network characteristics; and

updating the one or more lists of the one or more network characteristics of the plurality of messages, such that the one or more lists comprise instances of the one or more network characteristics based on at least a frequency of occurrences of the instances.

2. The method of claim 1, wherein the detecting comprises sniffing.

3. The method of claim 1, wherein the detecting comprises recording the plurality of messages.

4. The method of claim 1, wherein traveling near at least the first network node comprises traveling through the first network node.

5. The method of claim 1, wherein the first network node comprises a router.

6. The method of claim 1, wherein the plurality of messages comprise recursive messages.

7. The method of claim 1, wherein the plurality of messages comprise multipath messages.

8. The method of claim 7, wherein multipath messages comprise messages concurrently traveling to different nodes.

9. The method of claim 1, wherein the one or more network characteristics comprise one or more source addresses.

10. The method of claim 9, wherein the one or more source addresses comprise one or more Internet Protocol addresses.

11. The method of claim 1, wherein the one or more network characteristics comprise one or more destination addresses.

12. The method of claim 11, wherein the one or more destination addresses comprise one or more Internet Protocol addresses.

13. The method of claim 1, wherein the one or more network characteristics comprise one or more source ports.

14. The method of claim 13, wherein the one or more source ports comprise one or more Transmission Control Protocol ports.

15. The method of claim 13, wherein the one or more source ports comprise one or more User Datagram Protocol ports.

16. The method of claim 1, wherein the one or more network characteristics comprise one or more destination ports.

17. The method of claim 16, wherein the one or more destination ports comprise one or more Transmission Control Protocol ports.

18. The method of claim 16, wherein the one or more destination ports comprise one or more User Datagram Protocol ports.

19. The method of claim 1, wherein the one or more network characteristics comprise one or more flags.

20. The method of claim 19, wherein the one or more flags comprise Transmission Control Protocol flags.

21. The method of claim 19, wherein the one or more flags comprise Internet Control Message Protocol flags.

22. The method of claim 1, wherein the first packet network comprises at least one Asynchronous Transfer Mode network.

23. The method of claim 1, wherein the packet network comprises at least one Internet Protocol network.

24. The method of claim 1, wherein the frequency of occurrences comprises a number of occurrences in an amount of time.

25. The method of claim 1, wherein each of the one or more lists comprise a group of more frequently occurring instances of the one or more network characteristics

26. The method of claim 1, wherein each of the one or more lists comprise a group of most frequently occurring instances of the one or more network characteristics

27. The method of claim 1, wherein a number of instances in each of the one of more lists is substantially equal to or greater than a quotient, wherein the quotient comprises a router capacity rate divided by a threshold flooding rate.

28. The method of claim 1, wherein the first network node comprises at least a router.

29. The method of claim 1, wherein the plurality of messages comprises a plurality of Internet Protocol packets.

30. The method of claim 1, wherein the updating comprises updating at one or more nodes of the at least the first network node.

31. The method of claim 1, wherein the updating comprises updating at one or more nodes of at least a second network node.

32. The method of claim 31, wherein the second network node comprises at least a packet sniffer.

33. The method of claim 31, wherein the second network node comprises at least a router.

34. The method of claim 1, wherein the plurality of messages comprises a plurality of Asynchronous Transfer Mode cells.

35. The method of claim 1, wherein the detecting comprises recording the plurality of messages.

36. The method of claim 1, wherein traveling near at least the first network node comprises traveling through the first network node.

37. The method of claim 1, wherein the first network node comprises a router.

38. The method of claim 1, wherein the detecting comprises detecting at one or more nodes of the at least the first network node.

39. The method of claim 1, wherein the detecting comprises detecting at one or more nodes of at least a second network node.

40. The method of claim 39, wherein the second network node comprises at least a packet sniffer.

41. The method of claim 39, wherein the second network node comprises at least a router.

42. The method of claim 1, wherein the plurality of messages comprise multipath messages.

43. The method of claim 1, further comprising:

forwarding a message to at least a third network node;

responsive to receiving the message, updating a second plurality of one or more lists of a second plurality of one or more network characteristics of a second plurality of messages, such that the second plurality of one or more lists comprise a second plurality of instances of the second plurality of

one or more network characteristics based on at least a second frequency of occurrences of the second plurality of instances.

44. The method of claim 43, wherein the updating comprises updating at one or more nodes of the at least the third network node.

45. The method of claim 43, wherein the updating comprises updating at one or more nodes of at least a fourth network node.

46. The method of claim 43, further comprising:

forwarding a message to at least a fifth network node to update a third plurality of one or more lists of a third plurality of one or more network characteristics of a third plurality of messages, such that the third plurality of one or more lists comprise a third plurality of instances of the third plurality of one or more network characteristics based on at least a third frequency of occurrences of the third plurality of instances.

47. The method of claim 1, further comprising:

preventing a message from transiting the first network node, wherein the message comprises a suspicious instance matching at least one of the instances of the one or more network characteristics of the one or more lists.

48. The method of claim 47, wherein the suspicious instance comprises one or more source addresses associated with an attack.

49. The method of claim 48, wherein the one or more source addresses comprise one or more Internet Protocol addresses.

50. The method of claim 47, wherein the suspicious instance comprises one or more destination addresses associated with an attack.

51. The method of claim 50, wherein the one or more destination addresses comprise one or more Internet Protocol addresses.

52. The method of claim 47, wherein the suspicious instance comprises one or more source ports associated with an attack.

53. The method of claim 52, wherein the one or more source ports comprise one or more Transmission Control Protocol ports.

54. The method of claim 52, wherein the one or more source ports comprise one or more User Datagram Protocol ports.

55. The method of claim 47, wherein the suspicious instance comprises one or more destination ports associated with an attack.

56. The method of claim 55, wherein the one or more destination ports comprise one or more Transmission Control Protocol ports.

57. The method of claim 55, wherein the one or more destination ports comprise one or more User Datagram Protocol ports.

58. The method of claim 57, wherein the suspicious instance comprises one or more flags associated with an attack.

59. The method of claim 58, wherein the one or more flags comprise Transmission Control Protocol flags.

60. The method of claim 58, wherein the one or more flags comprise Internet Control Message Protocol flags.

61. The method of claim 47, wherein the preventing comprises filtering messages traveling the first packet network near the first network node.

62. The method of claim 47, wherein the preventing is responsive to receiving a message from an attacked network node.

63. The method of claim 62, wherein the attacked network node received a flooding attack.

64. The method of claim 62, wherein the attacked network node received a denial of service attack.

65. The method of claim 47, further comprising:

repeatedly updating of the one or more lists and removing, from the one or more lists, instances having a low frequency of occurrences; and

comparing the suspicious instance with the repeatedly updated one or more lists, and if the comparing fails to result in a match, halting the preventing.

66. The method of claim 65, wherein the halting the preventing comprises removing a filter, wherein the filter prevented messages comprising the suspicious instance from transiting the first network node.

67. The method of claim 1, further comprising:

receiving a message caused by an attacked network node.

68. The method of claim 67, wherein the message comprises a network identifier of the attacked network node.

69. The method of claim 67, wherein the message comprises a cookie generated by the attacked network node.

70. The method of claim 67, wherein the attacked network node received a flooding attack.

71. The method of claim 67, wherein the attacked network node received a denial of service attack.

72. The method of claim 67, wherein the attacked network node sent the message.

73. The method of claim 67, wherein an intermediate network node, coupled somewhere between the attacked network node and the node receiving the message, sent the message.

74. The method of claim 73, wherein the node receiving the message comprises the second network node.

75. The method of claim 73, wherein the node receiving the message comprises a third network node.

76. The method of claim 67, further comprising:

responsive to the receiving, comparing the instances of the one or more network characteristics with a suspicious instance comprised in the message caused by the attacked network node.

77. The method of claim 76, further comprising:

if the comparing results in a match, then forwarding, towards one or more suspect network nodes, the message comprising the suspicious instance, wherein each of the one or more suspect network nodes comprises one or more nodes that an attack on the attacked network node possibly transited to reach the attacked network node.

78. The method of claim 77, wherein the forwarded message comprises updated information.

79. The method of claim 77, wherein the updated information comprises a network identifier of a node forwarding the message.

80. The method of claim 76, further comprising:

if the comparing fails to result in a match, then sending, towards the attacked network node, a report message.

81. The method of claim 80, wherein the report message comprises a network identifier of a source of an attack on the attacked network node.

82. The method of claim 77, wherein the forwarding is based at least on at least one of the instances of the one or more network characteristics comprised in the maintained one or more lists.